4.1.16 Ensure system administrator actions (sudolog) are collected (Scored)

Profile Applicability

```
Level 2 - Server
Level 2 - Workstation
```

Description

Monitor the `sudo` log file. If the system has been properly configured to disable the use of the `su` command and force all administrators to have to log in first and then use `sudo` to execute privileged commands, then all administrator commands will be logged to `/var/log/sudo.log`. Any time a command is executed, an audit event will be triggered as the `/var/log/sudo.log` file will be opened for write and the executed administration command will be written to the log.

Rationale

Changes in `/var/log/sudo.log` indicate that an administrator has executed a command or the log file itself has been tampered with. Administrators will want to correlate the events written to the audit trail with the records written to `/var/log/sudo.log` to verify if unauthorized commands have been executed.

Audit

Run the following command and verify output matches:

```
# grep actions /etc/audit/audit.rules
-w /var/log/sudo.log -p wa -k actions
```

Remediation

Add the following lines to the `/etc/audit/audit.rules` file:

```
-w /var/log/sudo.log -p wa -k actions
```

Notes

The system must be configured with `su` disabled (See Item 5.6 Ensure access to the su command is restricted) to force all command execution through `sudo`. This will not be effective on the console, as administrators can log in as root.